IN THE CLAIMS:

Please amend claims 1-21 as follows.

1. (Currently Amended) Authentication method for a telecommunications network, comprising: ~~the method including the steps of~~

generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in a known mobile communications system; [,]

transmitting at least some of the challenges contained in the authentication data blocks to the terminal; [,]

choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system; [,]

determining an authenticator with an aid of the chosen key in the terminal; [,]

transmitting from the terminal to the network authenticator and a data unit, the data unit containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data unit of which key corresponding to which challenge was chosen, ~~and~~ a check value with the aid of the chosen key in the network; [,] and

comparing the check value with the authenticator.

2. (Currently Amended) Method as defined in claim 1, wherein the data unit is a SPI (Security Parameter Index) in the registration message of the mobile ~~IP~~ Internet Protocol ~~protocol~~.

3. (Currently Amended) The method ~~Method~~ as defined in claim 1, wherein the value of the response determined at the terminal is inserted into the data unit.

4. (Currently Amended) The method ~~Method~~ as defined in claim 1, wherein the challenges are sorted in an order at the terminal with the aid of predetermined sorting criteria and a consecutive number corresponding to the chosen challenge is inserted into the data unit.

5. (Currently Amended) The method ~~Method~~ as defined in claim 1, wherein the identification unit used in the terminal is the subscriber identity module used by the known ~~GSM~~ Global System for Mobile Communication system and the authentication data blocks are authentication triplets used by the ~~GSM~~ Global System for Mobile Communication system.

6. (Currently Amended) The method ~~Method~~ as defined in claim 5, wherein the authentication triplets are fetched from the authentication centre of the ~~GSM~~ Global System for Mobile Communication system.

7. (Currently Amended) The method ~~Method~~ as defined in claim 6, wherein the challenges to be transmitted to the terminal are transmitted by using a known short message switching service.

8. (Currently Amended) The method ~~Method~~ as defined in claim 1, wherein the challenges to be transmitted to the terminal are transmitted in an ~~IP~~ Internet Protocol datagram to be sent through an ~~IP~~ Internet Protocol network.

9. (Currently Amended) The method ~~Method~~ as defined in claim 1 for an ~~IP~~ Internet Protocol network, wherein the authentication data blocks are transmitted to the home agent of the terminal and with the aid of the data unit message is given to the home agent about which key corresponding to which challenge was chosen, whereby the check value is determined in the home agent.

10. (Currently Amended) An Authentication system for a telecommunications network, comprising: ~~the system including~~

in a terminal of the network, a first message transmission unit configured to transmit ~~means for transmitting~~ an authenticator and a data unit to the network, the data unit including information relating to the manner in which the authenticator is formed; [,] and

a checking unit configured to determined ~~means for determining~~ a check value with aid of the data unit,

wherein

the terminal of the network includes such an identification unit, which receives as input a challenge from which a response and a key are defined essentially in a same manner as in a subscriber identity module of a known mobile communications system,

the system includes a generating unit configured to generate ~~means for generating~~ authentication data blocks in the same manner as in the mobile communications system, the authentication data blocks include a challenge, a response and a key,

the system includes a transmission unit configured to transmit ~~means for transmitting~~ challenges contained by the authentication data blocks to the terminal, and

the terminal includes a selection unit configured to select ~~means for selecting~~ one challenge for use,

the first message transmission unit ~~means~~ insert such a value into the data unit which indicates which key corresponding to which challenge was selected for use in the terminal, and the first message transmission unit ~~means~~ determine the authenticator and the checking unit ~~means~~ determine the check value based on the selected key.

11. (Currently Amended) The system ~~System~~ as defined in claim 10, wherein the identification unit located in connection with the terminal is a subscriber identity module used in the mobile communications system.

12. (Currently Amended) The system ~~System~~ as defined in claim 10, wherein the said generating unit ~~means~~ include an authentication centre of the mobile communications system.

13. (Currently Amended) The system ~~System~~ as defined in claim 10, wherein the said transmission unit ~~means~~ include a unit ~~means~~ for carrying out a known short message switching service.

14. (Currently Amended) An authentication method for a telecommunications network, said method comprising:

generating a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key; [,]

transmitting at least some of the challenges contained in the authentication data blocks to a terminal; [,]

receiving an authenticator and a data unit containing information relating to a manner in which the authenticator is formed from the terminal; [,]

determining based on said data unit which challenge was chosen by the terminal; [,] and

determining a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

15. (Currently Amended) ~~An~~ The authentication method as defined in claim 14, wherein said data unit is a security parameter index in the registration message of a Mobile ~~IP~~ Internet Protocol protocol.

16. (Currently Amended) ~~An~~ The authentication method as defined in claim 14, wherein said data unit comprises the response corresponding to the chosen challenge.

17. (Currently Amended) ~~An~~ The authentication method for a terminal, said method comprising:

receiving a set of challenges from a telecommunications network; [,]

choosing one challenge from the set of challenges; [,]

determining a response and a key based on the chosen challenge; [,]

determining an authenticator based on the key corresponding to the chosen challenge; [,] and transmitting said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed; and

notifying the telecommunications network of the chosen challenge.

18. (Currently Amended) ~~An~~ The authentication method as defined in claim 17, wherein said data unit is a security parameter index in the registration message of a Mobile ~~IP~~ Internet Protocol protocol.

19. (Currently Amended) ~~An~~ The authentication method as defined in claim 17, wherein said data unit comprises the response corresponding to the chosen challenge.

20. (Currently Amended) A telecommunications network configured to:

generate a set of subscriber-specific authentication data blocks, each authentication data block containing a challenge, a response and a key; [,]

transmit at least some of the challenges contained in the authentication data blocks to a terminal; [,]

receive an authenticator and a data unit containing information relating to a manner in which the authenticator is formed; [,]

determine based on said data unit which challenge was chosen by the terminal; [,] and determine a check value with the key corresponding to the chosen challenge, said check value to be compared with the authenticator.

21. (Currently Amended) A terminal for a telecommunications network, said terminal configured to:

receive a set of challenges from a telecommunications network; [,]

choose one challenge from the set of challenges; [,]

determine a response and a key based on the chosen challenge; [,]

determine an authenticator based on the key corresponding to the chosen challenge; [,] and

transmit said authenticator and a data unit to the telecommunications network, said data unit relating to the manner in which the authenticator is formed and notifying the telecommunications network of the chosen challenge.

22. (Previously Presented) An apparatus of a telecommunications network, the apparatus comprising:

generating means for generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in a known mobile communications system;

transmitting means for transmitting at least some of the challenges contained in the authentication data blocks to the terminal;

choosing means for choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of an identification unit of the terminal essentially in the same way as in a subscriber identification module of the mobile communication system;

determining means for determining an authenticator with an aid of the chosen key in the terminal;

transmitting means for transmitting from the terminal to the network authenticator and a data unit, the data unit containing information relating to the manner in which the authentication is formed and notifying the network with the aid of the data unit of which key corresponding to which challenge was chosen, and a check value with the aid of the chosen key in the network; and

comparing the check value with the authenticator.